Lifecycle Business Process Compliance Management: A Semantically-Enabled Framework

Conference Paper · July 2015

DOI: 10.1109/CLOUDCOMP.2015.7149646

2 authors:

Amal Elgammal
Cairo University
48 PUBLICATIONS **710** CITATIONS
SEE PROFILE

Oktay Turetken
Eindhoven University of Technology
91 PUBLICATIONS **1,293** CITATIONS
SEE PROFILE

Lifecycle Business Process Compliance Management: A Semantically-Enabled Framework

Amal Elgammal
Faculty of Computers and Information
Cairo University, Egypt
Email: a.elgammal@fci-cu.edu.eg

Oktay Turetken
School of Industrial Engineering
Eindhoven University of Technology, Netherlands
Email: o.turetken@tue.nl

***Abstract*—Following the crisis in 2008, different industrial sectors has faced growing numbers of laws and regulations globally. The number and complexity of these regulations is creating significant issues for governance, risk and compliance management especially for heavily-regulated sectors, such as the financial industry. This paper proposes a semantically-enabled compliance management framework that backs up the entire business process compliance lifecycle, i.e., design-time verification, runtime and offline monitoring and analysis. In the heart of the framework is an integrated semantic repository incorporating domain, business and regulatory knowledge, at different levels of abstraction, which provides a shared conceptualization of the interrelated compliance and business specifics. Furthermore, given the technological evolution enabled by cloud computing, we draw our vision on providing compliance-related ontologies as a service (COaaS) on the cloud. As an initial validation step, we have considered the financial sector with an Anti-Money Laundering (AML) case study and applied our semantic-based approach on.**

Keywords— semantic BP compliance management; regulatory ontology;domain ontology; BP ontology; compliance patterns; ontology annotation; compliance ontology as a service

I. INTRODUCTION

The global regulatory environment has grown in complexity and scope since the financial crisis in 2008. This is causing significant problems for organizations in all industrial sectors, as the complexity of hard and soft regulations little understood or appreciated [1]. Take, for example, that the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 has an estimated 1,500 provisions and 398 rules, which are being drafted by relevant regulatory agencies—approximately 40% of these rules are in force in 2013. The U.S. Bank Secrecy Act Anti-Money Laundering (AML) rules are equally complex and far-reaching, with a raft of major banks found not to be in compliance in 2012. Standard Chartered Bank, London, for example, was fined a total of $459 million by U.S. regulators in December 2012. Worse still HSBC Holdings Plc. had pay a record $1.92 billion in fines to U.S. regulators for similar anti-money laundering offences.

In a broader perspective, compliance is about unambiguously ensuring conformance to a set of prescribed and/or agreed upon rules [2]. These rules may originate from various sources, including laws and regulations, standards, public and internal policies, partner agreements and jurisdictional provisions. To address this emergent *business need*, many organizations typically achieve compliance on a per-case basis resulting into myriad ad-hoc solutions. In practice, these solutions are generally handcrafted for a particular compliance problem, which creates difficulties for reuse and evolution. Furthermore, compliance and business concepts may be treated differently by different stakeholders. This ambiguity results in inconsistency, which makes it infeasible to share and re-use business and compliance specifics. All these problems make it infeasible for automated compliance checking and analysis at any of the phases of the BP lifecycle; design-time, runtime and off line monitoring.

In this paper, we draw our ongoing research to propose a generic semantically-based compliance management framework crosscutting and supporting the complete business process lifecycle; i.e. CMKB. The need to manage regulatory and compliance data, especially in heavily-regulated domains, exceeds the abilities of current information systems. Our research indicates that a framework for compliance management should be founded on a semantic knowledge base that incorporates and integrates a set of ontologies capturing the different perspectives of the compliance and business spheres. Therefore, in the heart of the framework is a uniform conceptualization of the process and compliance space, enabling the sharing and re-use of compliance and business knowledge, the elimination of any ambiguity, and improves the level of automation.

The semantic compliance management framework proposed in this paper is agnostic of the underlying adopted languages/technologies, and identifies the set of minimal ontologies that should exist for any solution attempts to address any of the compliance problems efficiently. Three main ontologies are identified as a mandatory: (i) *BP ontology*: an ontology capturing the semantics of the adopted BP language, e.g. BPMN, BPEL, (ii) *Domain Ontology*: an ontology representing the concepts and relationships that exist in the domain of interest, e.g., medical, transport, banking, aerospace, etc.

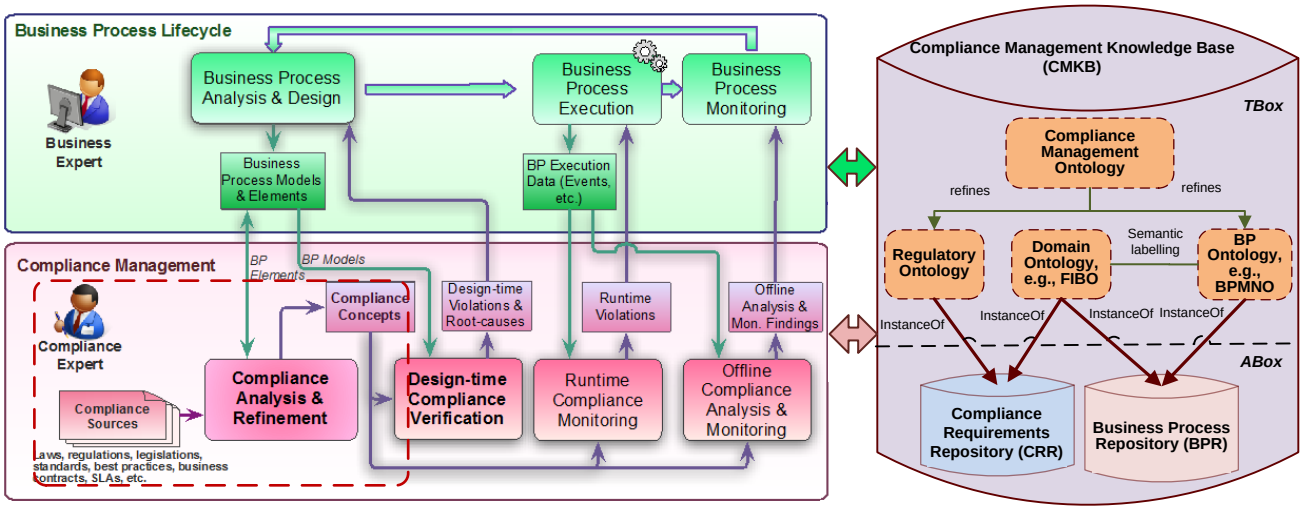

Fig. 1 Semantically-enabled compliance management framework

and (iii) *Regulatory Ontology*: an ontology formalizing the requirements, controls and rules of compliance imperatives. The semantic knowledge base also provides a high-level ontology that captures and links important high-level concepts of the business and compliance spheres; i.e., *compliance management ontology*, which is refined into the *BP ontology* and *Regulatory ontology*. Furthermore, given the technological revolution and advantages brought by cloud computing through the concept of utility computing, we also propose to host the different components of the CMKB on the cloud to enable the wide sharing and re-usability of compliance-related ontologies and cost-effective and rapid development of CMKB.

The rest of this paper is organized as follows: The semantic compliance management framework is presented in Section II. A simplified Anti-Money Laundering (AML) BP model related to the financial domain is presented in Section III and acts as a running scenario throughout this paper. We have developed this AML model based on the Financial Action Task Force (FATF) 40 recommendations[1]. Section IV and Section V details on the CMKB. The notion of COaaS is elaborated in Section VI. Related work is discussed in Section VII. Finally conclusions and future work are highlighted in Sections VIII.

II. Semantically-enabled Compliance Management Framework

Fig. 1 presents a high-level view of the semantically-enabled compliance management framework. There are two primary abstract roles involved: (i) a *business expert*, who is responsible for defining and managing BP in an organization, and (ii) a *compliance/legal expert*, who is responsible for refining, interpreting, specifying and managing compliance requirements in close collaboration with the business expert.

The right hand-side of Fig. 1 represents the CMKB, which is the backbone of the framework that incorporates and integrates a set of ontologies to capture the different perspectives of the compliance and business spheres. As shown in the left hand-side of Fig. 1, the framework is composed of two interacting main components; i.e., *business process lifecycle* and *compliance management*, each of which interacts continuously with the CMKB. CMKB is discussed in details next in Section V.

In the overall, the approach starts either with the BP lifecycle (the left upper-part of Fig. 1) or with compliance management practices (depicted in the left lower part of Fig. 1), which afterwards align and run together exchanging inputs and outputs. BP lifecycle starts with the analysis and design of the processes [1]. This involves the analysis of existing processes and the design of 'to-be' processes taking into account various factors, such as business objectives, risks, industry best practices and frameworks, and compliance requirements. Once these BP specifications are tested and have reached a steady state, they are deployed (e.g., on BP execution engines and other runtime environments) and executed. The BP executions are subsequently monitored by tracking the progress of individual process instances, so that statistics on their state and performance can be provided. Monitoring information and changes in the business environment may trigger another iteration of the BP lifecycle.

On the other side, compliance management practices commence with the *compliance analysis and refinement*, which involves, firstly, the analysis of the sources of compliance requirements, such as laws, regulations, standards, policies, etc. that state the norms mandating or impacting the way the business processes are executed;

.

[1]http://www.fatf-gafi.org/topics/fatfrecommendations/

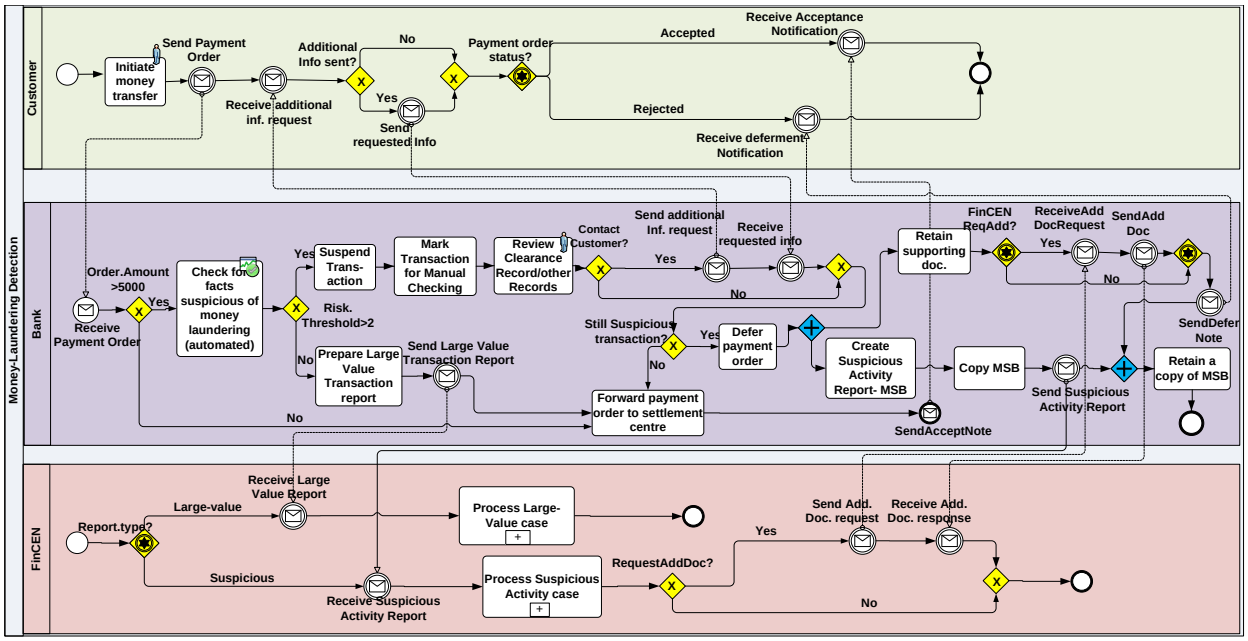

Fig. 2 Money laundering detection and reporting BPMN process

Secondly, it involves the transformation of these abstract norms into a set of concrete concepts relevant to compliance management. Analysis and refinement requires not only compliance but also BP domain knowledge. The key output of this step is the *compliance concepts* and their relationships that are stored and managed in the *compliance Requirements repository* of CMKB. We will elaborate on compliance refinement and internalization in Section IV.

The approach depicted in Fig. 1 encompasses three main compliance assurance activities each having a corresponding BP lifecycle stage and each is dependent on the semantic knowledge base; CMKB. *Design-time compliance verification* involves the static verification of business process models against formal compliance rules. Design-time compliance violations and possible root-causes provide key input for BP analysis and design activities to ensure that BP models progressing to execution are compliant by-design. Compliance checks at design-time are critical, as they are less costly than corresponding checks at later phases [2]. However, it is not always feasible to enforce compliance with all constraints imposed on a process models at design time. Therefore, *Runtime compliance monitoring* (i.e., verifying compliance dynamically during BP execution) and *offline compliance analysis and monitoring* (i.e., verifying compliance after BP execution) are vital for a holistic view ensuring compliance throughout the remaining phases of the BP life span.

This paper focuses on the topics that are relevant to the parts in Fig. 1 that are enclosed within dotted lines, i.e., (i) the compliance analysis and refinement, which represents the compliance step that handles the identification of concrete compliance concepts and populates the CMKB, and (ii) the semantic compliance management knowledge base, which incorporates a set of ontologies capturing different perspectives of the compliance and business spheres that: (i) supports the entire compliance management practices of Fig. 1; (ii) ensures their ontological alignment; (iii) eliminate ambiguities; (iv)facilities the communication between compliance and business experts; (v) and facilitates the re-use of compliance and business knowledge and their evolution and maintenance.

III. Money-Laundering Detection Process: Running Scenario

Anti-money laundering is a pressing concern to any organization operating in the financial industry, as it is tightly adjunct to terrorism and proliferation financing. Despite the fact that it is not possible to precisely quantify the amount of money laundered every year, in [3], it has been shown that billions of US dollars certainly are. As part of a previous work [4], we have built an end-to-end business process encoded in the BPMN v2.0 standard that captures money laundering detection and reporting of the AML practices. The BPMN model is established based on best practices and the Financial Action Task Force (FATF) 40 recommendations.

Fig. 2 presents the money laundering detection and reporting BPMN process. The process proceeds as follows: it starts by a customer initiating a money transfer. Once the order is received by the bank, and if the order amount is greater than a given threshold (interpreted as 5k Euros in our BPMN model), an automated check is carried out to detect if the transaction is suspicious. If the automated module detects that the transaction is suspicious, an authorized personnel is required to re-check the transaction manually by reviewing clearance records and all other available records, and contacting the customer for further information, if necessary.

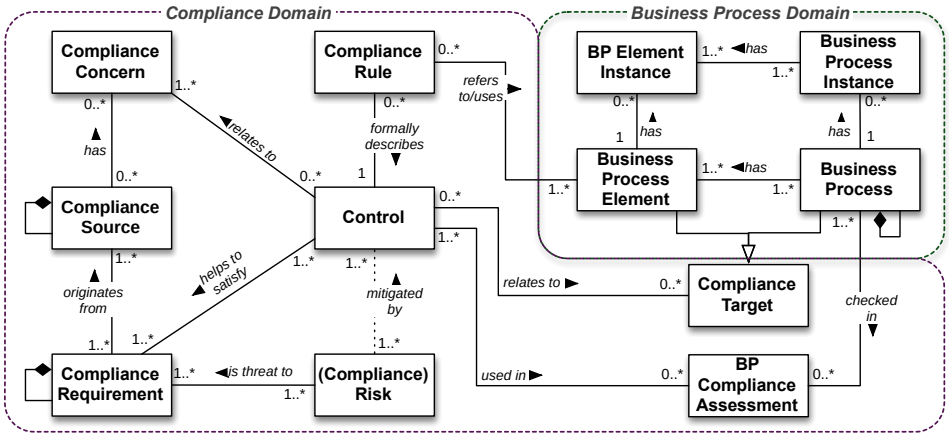

Fig. 3 Key concepts of the compliance management ontology

If the transaction is proved to be suspicious, the transaction is flagged as suspicious and then deferred, and a Suspicious Activity Report (MSB) is sent to FinCEN[2]. The customer will be notified in both cases on the status of her transaction, while retaining all supporting documents in case they are requested by FinCEN during its investigation.

IV. Refining and Internalizing Compliance Constraints

Compliance sources are often abstract, complex and ambiguous. As a result they typically require expert interpretation and translation to concrete and organization-specific requirements. There are only few approaches that guide organizations to advance through this refinement process. We introduced in [5, 6] a brief approach based on the COSO framework [7], which is recognized by regulatory bodies as a de facto standard for establishing internal control systems. The approach involves the following major steps:

1. Analyse and interpret compliance sources in order to identify and elucidate the requirements with which the organization has to comply. These sources prescribe requirements in a range of abstraction levels from vague compliance constraints to precisely described controls.
2. Perform a 'risk assessment' to identify the risks to the achievement of these compliance requirements.
3. Design actions/statements (referred as 'controls') to mitigate the compliance risks identified.
4. Use *patterns* to represent controls and generate (formal) rules for those controls that can be realized with a formal language and be effectively used for automated compliance assurance.

As organizations typically deal with a number of diverse compliance sources, there is a need for a structured means for capturing and organizing compliance information and their interrelationships to support business and compliance experts particularly in the compliance analysis and refinement process. The *compliance management ontology* shown in Fig. 1 is geared towards filling in this gap.

[2] Financial Crimes Enforcement Network: http://www.fincen.gov/

Compliance management ontology provides a generic and comprehensive structure tailored for compliance concepts and their relation to business processes, and establishes the underpinnings of the semantic BP compliance management approach depicted in Fig. 1. The proposed ontology clearly separates two domains -business processes and compliance- while establishing their relation and traceability. Managing the traceability mainly involves tracing compliance requirements *back* to their sources, or *forward* to the processes that enforce them [8]. Bi-directional traceability is important as it helps to recognize the implications of changing requirements and processes. It allows analyzing why a particular decision in a process was made and what the implications of changing these specifics are in relation to the compliance requirements. In the following, we describe the key constructs both in the business process and compliance domains in line with the refinement approach we depict above.

03

N. Long Ha

As shown in Fig. 3, we assume a *generic* model for the BP domain in order for the proposed model not to be constrained for a particular BP modelling notation. We assume *business processes* are designed as a collection of *process elements*. An organization might want to capture different aspects of their processes. Depending on these aspects, process elements may take diverse forms including the *basic elements*, such as activities, events, and business objects; *and others*, such as roles, org. units, software systems, and goals. Business processes and process elements are instantiated during process execution to achieve process goals. These instantiations are also subject to compliance requirements (through the elements they are instantiates from) as many of these requirements are dependent on runtime conditions.

A *compliance source* is the origin of compliance requirements. It can be in the form of a regulation, legislation or law, such as SOX [9], HIPAA [10]; standards or code of practices, such as ISO/IEC 27000 [11] series; internal or external policies; or business partner contracts. A source typically consists of a set of sections or clauses in a hierarchical form. Interpretation of these sources results into *compliance requirements* expressed at various abstraction levels.

TABLE 1 EXCERPT OF COM. REQ. RELEVANT TO THE AML SCENARIO

ID	Control	Comp. Req.	Risk	Comp. Source
C1	It is obligatory that the financial institution reports any suspicious transaction that involves or aggregates funds of at least $5,000	Identity Reporting related provisions	- Fraud/misuse - Financial loss -Anti-money Laundering -Terrorism financing	US Patriot Act. § 1022.210 § 1022.320
C2	It is necessary that customer identification and verification includes name, date of birth, address and identification number of a person			
C3	It is obligatory that the identification of a suspicious transaction is from a review of clearance record or other record of money order that are sold and processed			
C4	It is obligatory that the customer gets notified by either the acceptance or deference of the money order	Transparency of the transaction	- Loss of customers -loss of reputation	- Internal Policy
C5	It is obligatory that each suspicious activity report is confidential and any information about the suspicious activity report is confidential	Confidentiality of money order	- Legal penalty due to non-compliance with laws	US Patriot Act. § 1022.320 (d)

A compliance requirement is a constraint or assertion that prescribes a desired result or purpose to be achieved by factoring actions or control procedures in processes. It can be prescribed in the form of abstract constraints or control objectives [12].

Performing risk assessment to identify the *risks* influencing the achievement of these requirements/objectives is one of the key components of compliance management. A *risk* is the probability of occurrence of an event that might influence the achievement of certain goals [13], which in turn might impair the organization's business model, reputation and/or financial condition. A risk is usually measured as a combination of impact and probability of occurrence [12]. Risk assessment also generates a set of *(internal) controls* to *mitigate* the risks and to ensure an effective implementation of the compliance requirements [7]. A *control* describes the restraining or directing influence to check, verify or enforce rules to satisfy one or more compliance requirements. Failure to address controls increases the likelihood of a (*compliance) risk* to materialize. Controls are typically concrete and organization-specific.

Table 1 presents a selection of the compliance requirements and core concepts instantiation including risks, controls and sources applicable to the suspicious transaction reporting scenario that we introduced in Section III.

Controls are related to different aspects of compliance and can be grouped into *compliance concerns*, such as security, privacy, segregation-of-duties, access-rights/authorizations, management reviews, etc. Concerns often crosscut business processes. A compliance source may enforce controls in diverse concerns, and solutions addressing a certain concern usually handle relevant controls in similar ways.

A key *touchpoint* between the compliance and the business process domains is the link between the controls and the compliance targets (as shown in Fig. 3). A compliance target is an abstract concept representing a generic 'object' of compliance requirements. They are in the form of business processes or process elements. A control applies to compliance targets and their properties. A BP compliance *assessment* is performed to verify and ascertain that an organization is designing and executing processes that satisfy the compliance requirements applicable them. It involves checking (during design-time, runtime, and offline) whether a set of compliance targets conforms to applicable rules with the purpose of identifying if and how a target can be changed to make it (more) compliant.

Compliance management ontology is a high-level ontology capturing compliance and business concepts and their relationships. To be able to represent in more detail concepts such as 'Compliance Rule' and 'Business Process Elements', which is necessary for future automated reasoning and verification assurance stepts, we refined *compliance management ontology* into a set low-level ontologies, which enables the concrete formalization of controls/rules, and their verification against BPMN models. Details are given next in Section V.

V. COMPLIANCE MANAGEMENT KNOWLEDGE BASE

The right hand-side of Fig. 1 represents the CMKB, highlighting one of the main contributions of this paper. The CMKB knowledge base represents the backbone of the framework, which incorporates and integrates a set of ontologies to capture the different perspectives of the compliance and business spheres. Compliance management ontology as a high-level ontology capturing generic compliance and business process concepts and their relationships has been discussed in Section IV, which is the basis of compliance requirements refinement and internalization discussed in the same section.

On a fine-grained perspective, Compliance management ontology is then refined into a more detailed representation of the regulatory and business process domains. More specifically, three main ontologies are needed: (i) *BP ontology*: an ontology capturing the semantics of the adopted BP language, e.g. BPMN, BPEL, (ii) *Domain Ontology*: an ontology representing the concepts and relationships that exist in the domain of interest, e.g., medical, transport, aerospace, etc. and (iii) *Regulatory Ontology*: an ontology formalizing the requirements, controls and rules of compliance imperatives. Ontologies in CMKB may be represented formally in the Ontology Web Language (OWL2.0). We build upon the BPMNO ontology [14] as the BP ontology. BPMNO provides a rich ontological representation of the BPMN v2.0 [15] standard. Moreover, we utilize the Financial Industry Business Ontology (FIBO) [16] as the domain ontology since the case study we use in this paper (and introduced in Section III) concerns with the financial domain.

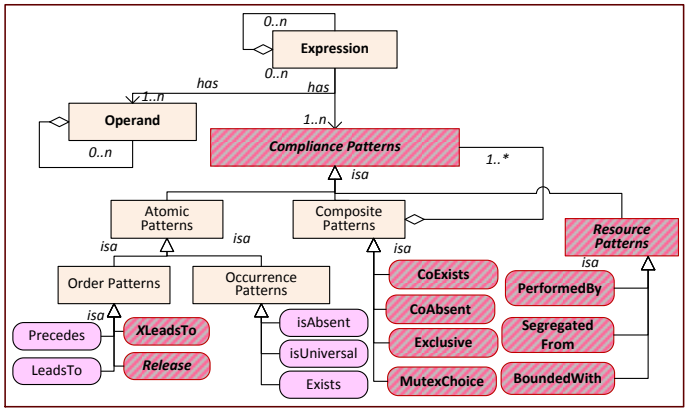

Fig. 4 Compliance Request Language (CRL) meta-model (core) [17]

06

N. Long Ha

FIBO[3] is an adopted OMG standard, a collaborative initiative led by industry members of the Enterprise Data Management Council (EDMC) in collaboration with the Object Management Group (OMG). FIBO aims at bridging the language gap between business and technology by capturing business meanings, rather than being a mere data dictionary. FIBO constitutes a set of formal models that define unambiguous shared meaning for financial industry concepts. The main components of FIBO are: (i) a Business Conceptual Ontology (FIBO-BCO), (ii) a web-accessible business presentation layer, (iii) a set of operational ontologies, and (iv) the FIBO Object Management Group Specifications. The web-accessible business presentation layer is the EDM Council Semantics Repository. It presents FIBO-BCO, alongside its OWL representation, in a business readable format that avoids technical representations or the need to learn new languages.

In a green scenario, if a BPMN process to be built from scratch, concepts and relations from FIBO can be directly used to guide its design and development. However, if BP models already exist (which is the common case), concepts from FIBO can be used to provide semantic annotation to existing BPMN models, and various reasoning mechanisms could be applied to ensure the correctness of these annotations as proposed in [14]. Examples of concepts in FIBO are: 'Agent', 'Person', 'National id', 'real estate', 'agreement, contract', 'ownership', 'Asset', etc.; examples of relations are: 'manages', 'provides', 'represents', 'is issued by', 'is appointed by', etc. Examples of concepts in BPMNO are: 'Activity', 'Event_types', 'Task', 'Gateway', etc.

Regulatory ontology is under development that addresses the regulatory domain by capturing concepts and relationships necessary to represent compliance rules that formally describe controls (cf. Fig. 3). Key concepts in this ontology are 'Input Data', 'Events', 'Condition', 'Action', 'Boolean Operator', etc. Following Step 4 of the compliance refinement methodology introduced in Section IV, *patterns* may be used to capture controls that are subject to automated verification and analysis. into the low-level and complex details of the underlying formal language.

[3] FIBO: http://www.omg.org/hot-topics/fibo.htm

TABLE 2 USING CMKB TO CAPTURE SOME AML CONTROLS

ID	Concepts from CMKB	Textual CRL
C1	Action, Condition, Input Data, Boolean Operator, Occurrence Patterns	(Order.Amount > 5000 ***And*** StillSuspiciousTransaction = 'Yes') ***LeadsTo***(SendSuspiciousActivityReport)
C3	Action, Condition, Input Data, Boolean Operator, Occurrence Patterns	(ReviewClearanceRecord ***And*** ReviewClearanceRecord.Manual = 'Yes') ***Precedes*** (SendSuspiciousActivityReport)
C4	Action, Occurrence Patterns, Composite Patterns	InitiateMoneyTransfer ***LeadsTo*** (SendAcceptNote ***MutexChoice*** SendDeferNote)

The usage of patterns is mainly to provide an abstraction layer, so that experts do not have to go into the low-level and complicate details of the underlying formal/logical language. Compliance Request Language (CRL) [17] is an expressive and rich compliance pattern specification language that covers the four structural facets of BPs; i.e., control-flow, data, employed resources and real-time. Our regulatory ontology is being developed to formalize CRL in OWL (Fig. 4 presents a subset of the core concepts and relationships of the CRL). Therefore, the Regulatory ontology also maintains concepts such as 'Compliance Patterns', 'Occurrence Patterns', 'Timed Patterns', 'Operand', 'Label', etc.

As shown in Fig. 1, Compliance Management Ontology, BP ontology (BPMNO), Domain Ontology (FIBO) and Regulatory ontology represent the Terminological part (TBox) of the CMKB. Instances from these ontologies populate the Compliance Requirements Repository (CRR), and Business Process Repository (BPR), representing the Assertional part (ABox) of the knowledge base. Table 2 presents how controls C1, C3 and C4 from Table 1 are represented as patterns (in textual format just for illustration purposes), using concepts and relationships from CMKB. Concrete actions names, data conditions are coming from FIBO and BPMNO (Due to space limitation, only controls C2, C5, C6 of Table 1 are omitted).

In the next Section, we draw our ideas on hosting and merging the different components of the CMKB as a service on the cloud, following a multi-cloud platform, for a better re-usability and cheaper/faster deployments.

VI. COMPLIANCE ONTOLOGY AS A SERVICE (COAAS)

Cloud computing allows computing services/resources to be provided as utilities over a network, usually the internet [18]. The traditional cloud stack mainly includes three layers: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Customers are charged for these services based on their usage. Cloud computing is rapidly evolving and is considered as a revolution in the computing practices through the concept of utility computing, which is cost effective and enables fast and efficient deployments. Following this technological revolution, everything is now offered on the cloud as a service; i.e., Everything-as-a-Service (XaaS), such as storage as a service (SaaS), communications as a service (CaaS), and monitoring as a service (MaaS).

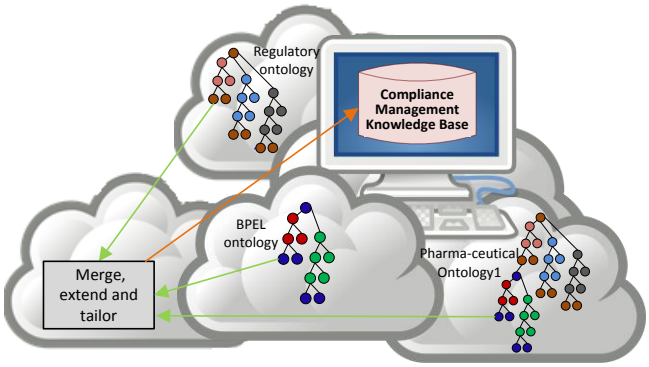

Fig. 5 An example of COaaS

In this paper, we propose to host the different ontologies of the CMKB discussed in SectionIV and Section V as a service (cf. Fig. 1), i.e., Compliance Ontologies as a Service (COaaS). As illustrated in Section II, the knowledge base constitutes three main ontologies: (i) Domain Ontology, (ii) BP Ontology, and (iii) Regulatory ontology. Regulatory ontology can be used for most application domains; however, domain and BP ontologies need to be concretized. For example, in this paper, we have used FIBO as the domain ontology to represent the financial sector, and we have also considered BPMN business process language.

Current cloud technology follows a single service provider centric model, such that one service is provided by one provider. As witnessed in [19, 20] , in the near future, there is a second wave of cloud computing, which allows multi-cloud providers to provide an interoperable services to customers. Following this wave, we propose that ontologies that build up the CMKB be composed/merged from different cloud vendors based on the specific application domain and the business process modelling/execution language used, which we call COaaS. For example, as shown in Fig. 5, in a pharmaceutical application assume that it adopts BPEL as the BP execution language, a BPEL ontology may be hosted by provider1, the pharmaceutical domain may require two ontologies, which are hosted by provider2 and provider3,and Regulatory ontology is hosted by provider4. In order to build the CMKB of this application, services from these providers need to be merged, extended and tailored to the specific needs of the application. This work direction is ongoing work, where merging techniques from [19] and the applicability and utility of this approach needs to be explored and validated.

VII. Related Work

With the increase in attention paid to the role of compliance in organizations, several work efforts have been produced in the area of compliance management, attempting to address the current needs of organizations. The main contribution of this paper is providing a set of business and compliance ontologies as the backbone of any compliance solution; CMKB, which provides a shared conceptualization of the compliance domain. This has the advantages of: (i) the CMKB serves as a communication between compliance and business experts, (ii) removes any ambiguity and is the foundation of the next verification, monitoring and analysis activities crosscutting and supporting the complete BP lifecycle and (iii) it facilities the re-use and sharing of knowledge, and assists its evolution.

An influential stream of research proposes to use semantic technologies to model the business and compliance space and possibly check the satisfaction of some *structural* compliance constraints. Semantic technologies have the main objective of providing a uniform representation of an organization process space at a semantic level mainly for knowledge sharing and reusability. The core idea is to use an ontology language, e.g. the Ontology Web Language (OWL) standard to represent relevant process and compliance concepts and their intricate relationships. OWL is formally grounded on Description Logic (DL). OWL associated automated reasoning tools, e.g. FaCT++, Pellet, may then be used to check the compliance. Prominent work efforts in this direction are [21], [22], [14] and [23]. However, as pointed out in [14] ontology languages, such as OWL and DL can only capture the structural part of a specific domain. They are not particularly suited to capture the dynamic behaviour, which concerns itself with how the flow proceeds within a process. Behavioural aspects can be better captured using formal languages for workflow, such as petri-nets and state machines.

The study in [24] proposes a compliance ontology, CoMOn, only focusing on the regulatory domain, while the concept of compliance patterns is not included and domain ontology is not considered. In [25], a policy and rule ontologies are proposed based on Event-Condition-Action, however the CMKB proposed in this paper is more comprehensive, agnostic of the underlying language/technology, and advocates the importance of the specific domain knowledge to address any compliance problem.

CMKB constitutes a number of ontologies at different levels of abstraction, which captures mandatory perspectives of the compliance and business spheres, and is necessary to provide a sematic dimension to any compliance solution. CMKB can be used as the backbone of any compliance solution that crosscuts the business process lifecycle; design-time, runtime and offline monitoring and analysis. An integral part of CMKB is the specific domain's knowledge, e.g., healthcare, aerospace, etc., which is key for any compliance solution to work efficiently in practice. Furthermore, we propose the notion of Compliance Ontologies as a Service (COaaS), such that different compliance-related ontologies can be hosted on the cloud, and following a multi-cloud providers approach, relevant ontologies can be discovered, extended, merged and tailored to the specific application needs.

VIII. Conclusions and Future Work

Business process compliance management is an emergent *business need*, as it has been witnessed that without explicit BP definitions, effective and expressive compliance frameworks, organizations may face litigation risks and even criminal penalties. This is particularly challenging for organizations operating in highly-regulated environments and governed by large number of regulatory requirements,

which raise many complex research and development problems.

This paper contributes by an integrated semantic compliance management framework, which can serve as the basis of any compliance solution crosscutting the complete business process lifecycle; design-time, runtime and offline monitoring and analysis. CMKB provides a uniform *conceptualization* of the regulatory and business compliance space, enables the sharing and reusability of this knowledge, and improves the level of automation, removes any ambiguity and significantly facilitates the communication between different stakeholders. CMKB adopts the notion of compliance patterns, and the proposed regulatory ontology captures the concepts and relationships of the compliance request language (CRL) [17], as a rich and expressive pattern-based compliance specification language. CMKB considers the specific domain's knowledge as key component of the approach.

Given the technological revolution and advantages brought by cloud computing, we also propose to host the different components of CMKB on the cloud to enable the wide sharing and re-usability of compliance-related ontologies. This enables cost-effective and rapid development of CMKB. Based on the specific application's needs, relevant ontologies capturing the business domain, the business process modelling/execution language and regulatory domain will be discovered, extended, merged and tailored to fit the specifics of this particular application. Our work in this direction is still ongoing.

Future work will involve the full implementation and integration of the proposed ontologies in OWL, and the evaluation and validation of the semantic-based approach by integrating it to compliance solutions at the three phases of the business process lifecycle; i.e., design-time, runtime and offline monitoring. As an initial validation step, in [4] we have integrated a preliminary version of the CMKB with the design-time compliance management approach in [17]. The findings have shown that the integration could be achieved smoothly, and assists the formalization and verification of corresponding compliance constraints on the basis of a shared conceptualization. It also significantly facilitates the communication between legal and compliance experts. Future efforts will also involve the integration of CMKB with the runtime compliance monitoring approach in [26], for a lifetime semantically-enabled compliance support.

REFERENCES

[1] M. P. Papazoglou and W.-J. v. d. Heuvel, "Business process development life cycle methodology," *Commun. ACM*, vol. 50, pp. 79-85, 2007.

[2] L. Ly, S. Rinderle-Ma, K. Göser, and P. Dadam, "On enabling integrated process compliance with semantic constraints in process management systems," *Information Systems Frontiers*, pp. 1-25, 2009.

[3] P. Reuter and E. M. Truman, *Chasing Dirty Money: The Fight Against Money Laundering*, 2004.

[4] A. Elgammal and T. Butler, "Towards a Framework for Semantically-Enabled Compliance Management in Financial Services," in *1st International Workshop On Knowledge Aware Service Oriented Applications in conjunction with ICSOC'14*, France, 2014.

[5] O. Turetken, A. Elgammal, W.-J van den Heuvel, and M.P. Papazoglou. (2012) Capturing Compliance Requirements:A Pattern-Based Approach. *IEEE Software, special issue on Software Engineering for Compliance*, vol. 29 No. 3, pp. 28-36.

[6] O. Turetken, A. Elgammal, W. J. van den Heuvel, and M. Papazoglou, "Enforcing Compliance on Business Processes through the use of Patterns," presented at the 19th European Conference on Information Systems (ECIS 2011), Finland, 2011.

[7] COSO, "Internal Control – Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission," ed, 1994.

[8] G. Koliadis and A. K. Ghose, "Service Compliance: Towards Electronic Compliance Programs," Tech. Rep. TR2008-01, Decision Systems Lab, University of Wollongong2008.

[9] SOX, "Sarbanes-Oxley Act of 2002, U.S. Congress," ed, 2002.

[10] HIPAA, "The Health Insurance Portability and Accountability Act, U.S. Congress," ed, 1996.

[11] ISO/IEC, "ISO/IEC 27000:2009 - Information security management systems — Overview and vocabulary," ed, 2009.

[12] COBIT, "Control Objectives for Information and related Technology - COBIT, 4.1. IT Governance Institute.," ed, 2007.

[13] S. Strecker, D. Heise, and U. Frank, "RiskM: A multi-perspective modeling method for IT risk assessment," *Information Systems Frontiers*, pp. 1-17, DOI: 10.1007/s10796-010-9235-3., 2010.

[14] C. Di Francescomarino, C. Ghidini, M. Rospocher, L. Serafini, and P. Tonella, "Reasoning on Semantically Annotated Processes," in *International Journal of Service Oriented Computing (ICSOC)*, Australia, 2008, pp. 132-146.

[15] OMG, "Business Process Model and Notation (BPMN), Version 2.0," ed, 2011.

[16] M. Bennett, "The financial industry business ontology: Best practice for big data," *Journal of Banking Regulation*, vol. 14, pp. 255-268, 2013.

[17] A. Elgammal, O. Turetken, W. J. van den Heuvel, and M. P. Papazoglou, "Formalising and Appling Compliance Patterns for Business Process Compliance," *Journal of Systems and Software Modelling (SoSym)*, 2014.

[18] M. Michael, *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online*: Pearson Education, 2011.

[19] A. Flahive, D. Taniar, and W. Rahayu, "Ontology as a Service (OaaS): a case for sub-ontology merging on the cloud," *The Journal of Supercomputing*, vol. 65, pp. 185-216, 2013.

[20] T. Velte, A. Velte, and R. Elsenpeter, *Cloud Computing, A Practical Approach*: McGraw-Hill, Inc. , 2010.

[21] F. Thomas, "Constructing Legal Arguments with Rules in the Legal Knowledge Interchange Format (LKIF)," presented at the Computable Models of the Law, Languages, Dialogues, Games, Ontologies, 2008.

[22] M. Hepp and D. Roman, "An Ontology Framework for Semantic Business Process Management," *Business and Information Systems Engineering- BISE (Wirtschaftsinformatik)*, 2007.

[23] P. De Leenheer, J. Cardoso, and C. Pedrinac, "Ontological Representation and Governance of Business Semantics in Compliant Service Networks," in *4th International Conference on Exploring Service Science*, Porto, 2013, pp. 155-169.

[24] N. Syed Abdullah, S. Sadiq, and M. Indulska, "A Compliance Management Ontology: Developing Shared Understanding through Models," *Advanced Information Systems Engineering*, vol. 7328, pp. 429-444, 2012.

[25] M. Elkharbili, S. Stein, and E. Pulvermüller, "Policy-Based Semantic Compliance Checking for Business Process Management," in *MobIS Workshops*, 2008, pp. 178-192.

[26] A. Awad, A. Barnawi, A. Elgammal, R. Elshawi, A. Almalaise, and S. Sakr, "Runtime Detection of Business Process Compliance Violations: An Approach Based on Anti Patterns," in *The 12th Enterprise Engineering Track At Acm Sac'15*, Spain, 2015.

Lifecycle Business Process Compliance Management: A Semantically-Enabled Framework

Elgammal, Amal; Turetken, Oktay

01 N. Long Ha Page 2
26/3/2022 9:26

02 N. Long Ha Page 2
26/3/2022 9:26

03 N. Long Ha Page 5
26/3/2022 9:26

04 N. Long Ha Page 6
26/3/2022 9:26

05 N. Long Ha Page 6
26/3/2022 9:26

06 N. Long Ha Page 7
26/3/2022 9:26

07 N. Long Ha Page 9
26/3/2022 9:26